Configuring GTA Firewalls for Remote Access

IPSec Mobile Client, PPTP and L2TP

RA201203-04

Global Technology Associates, Inc.

Global Technology Associates
3505 Lake Lynda Drive Suite 109
Orlando, FL 32817

Tel: +1.407.380.0220
Fax. +1.407.380.6080
Email: info@gta.com
Web: www.gta.com

Table of Contents

IPSec Mobile Client

IPSec Mobile Client Requirements

- Mobile IPSec Client License
- IPSec Client (Shrew Soft VPN Client for Windows and Linux or IPSecuritas IPSec Client for Mac)
- GB-OS 5.3.1 or higher

Running the IPSec Wizard

The IPSec Setup Wizard is designed to help configure a simple Virtual Private Network (VPN). The wizard will automatically create security policies to accept connections using ESP (protocol 50) and UDP (ports 500 and 4500) protocols.

Note

All connections through the VPN are controlled by VPN policies, located at **Configure>Security Policies>Policy Editor>IPSec**.

IPSec Setup for a Mobile IPSec VPN Client

1. The first screen of the wizard will prompt you to enter a brief description of the nature of the VPN.
   a. Enter a description for the VPN. For example, `Orlando to New York`.
   b. Select the Remote Type from the dropdown menu. Select Mobile Client.
   c. Click the Next Arrow to continue.

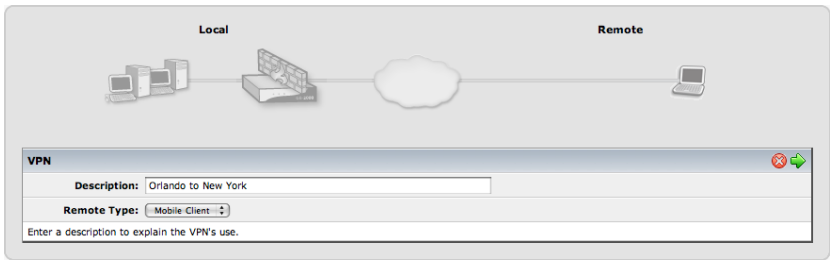

Figure 1.1: *Entering the VPN's Description*

2. The following screen will be used to define the Remote Network - where the Mobile IPSec VPN Client will be connecting from.
   a. Enter the Mobile IPSec VPN Client's IDENTITY and FULL NAME in the appropriate fields. The IDENTITY must be in the form of an email address.
   b. Enter a password. The password is used to ensure a secure, trusted connection between host computers and the internal network.
   c. Set the GROUP to **<Users>** or a pre-defined group with Mobile IPSec VPN enabled.
   d. Click the **NEXT ARROW** to continue.

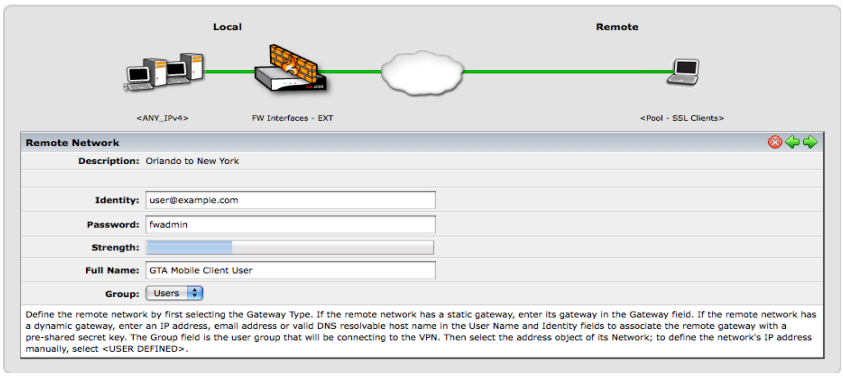

Figure 1.2: *Defining the Remote Network (Mobile Client)*

3. The final screen of the IPSec Setup Wizard is a summary view of all entered settings. Please review the VPN's setup prior to committing the displayed configuration. To make changes to your basic setup, select the **Back** button to return to the appropriate screen.

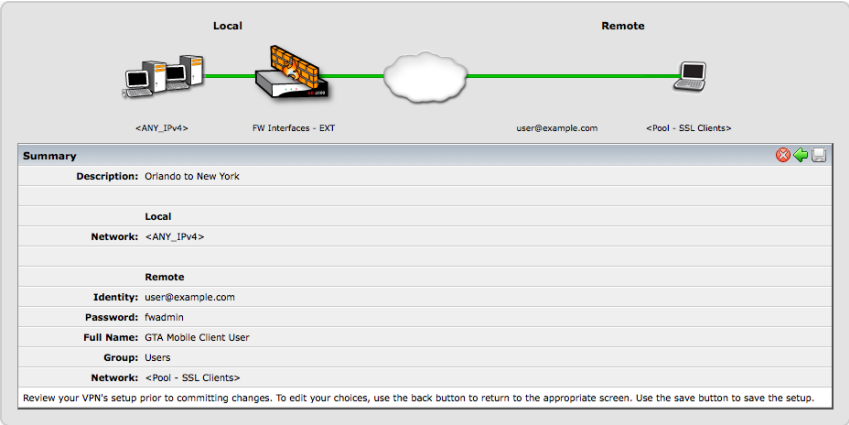

Figure 1.3: *Review VPN Configuration*

4. Click the **Save** icon to save the displayed configuration, or select the **Cancel** icon to abort. Saving the configuration will insert a new user on the firewall. A pop up will also display, prompting the download of the new configuration file.

Firewall Configuration

Configuring the firewall for Mobile IPSec Clients involves six (6) steps:

1. Create a Certificate Authority (CA) certificate
2. Define a group
3. Define a user
4. Configure address objects
5. Configure the Mobile IPSec Client
6. Configure security policies

After configuring the firewall, the Mobile IPSec Client can be installed. Please see the specific Windows, Linux, and Mac OS guides for installing the Mobile IPSec Client.

Creating a Certificate Authority (CA) Certificate

Create a Certificate Authority (CA) Certificate to sign all other Certificates.

1. Navigate to **Configure>VPN>Certificates**.
2. Set the section to default. The firewall will automatically generate a new CA and Remote Administration certificate, and assign them as CA, Remote Administration, and VPN certificate. Below is an example of the CA, Remote Administration, and VPN certificates.

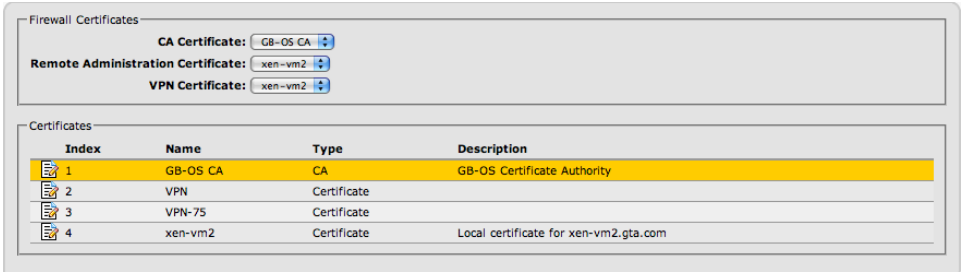

Figure 1.4: *Creating Certificates*

Note

If the firewall's VPN certificate is updated and it is used in a Site to Site IPSec Tunnel, the remote firewall will need to have the updated certificate.

If a user's certificate is updated and they use an SSL VPN, IPSec RSA, or IPSec RSA+XAuth VPN configuration they will need to download new VPN configurations.

See the *GB-OS Certificate Management Guide* for more information on firewall certificates.

Defining a Group

1. Navigate to **Configure>Accounts>Groups**.
2. Create a NEW group, or edit an existing group.
3. Enable Mobile IPSec.
3. Click **OK** and save section.

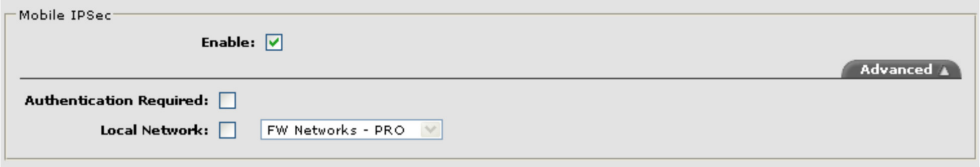

Figure 1.5: *Defining a Group*

Table 1: Defining Groups		
Field	**Default**	**Description**
Disable	Unchecked	Disables the group.
Name	Blank	Name used to reference the group for permissions.
Mobile IPSec		
Enable	Unchecked	Enables IPSec Client connections for the group.
Advanced		
Authentication Required	Unchecked	User must authenticate using GBAuth prior to establishing the VPN.
Local Network	Unchecked	Override for local network configured in **Configure>VPN>Remote Access>IPSec**.

Defining Users

1. Navigate to **Configure>Accounts>Users.** Create a **NEW** user or **EDIT** an existing user.
2. Select the Mobile IPSec group previously configured.
3. Assign the VPN certificate previously defined or generate a new certificate.
4. Enter the password the user will use to login to the IPSec Mobile Client.
5. Enable Mobile IPSec by leaving the **DISABLE** button unchecked.
6. Select HYBRID + XAUTH authentication.

Note

User certificates used for the IPSec Client MUST be signed by a CA.

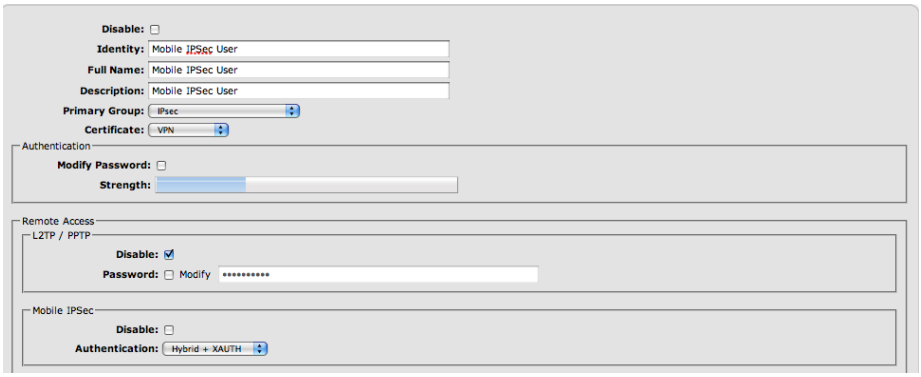

Figure 1.6: *Defining Users*

Table 2: Defining Users		
Field	**Default**	**Description**
Disable	Unchecked	Disables the user.
Identity	Blank	The name used to authenticate the connecting user. This must be a unique name. Minimum of three (3) characters.
Full Name	Blank	Name to identify the user. Minimum of three (3) characters.
Description	Blank	User defined description for the user.
Primary Group	Users	Primary group for specifying the type of access allowed for the IPSec Client. Also used in security policies for authentication.
Certificate	Generate	Generate automatically creates a user certificate based on user definition, or select a predefined certificate.
Authentication		
Password	Blank	Password for user to authenticate with the firewall. Minimum of four (4) characters.
Remote Access		
L2TP / PPTP		
Disable	Checked	Uncheck to enable PPTP or L2TP for the user.
Password	Blank	Password for user PPTP or L2TP access. Minimum of four (4) characters.
Mobile IPSec		
Disable	Checked	Uncheck to enable Mobile IPSec for the user.
Authentication	Hybrid + XAUTH	The authentication method the user MUST use for IPSec VPN. Options include Hybrid + XAUTH (password required); Pre-Shared Key (authenticated via pre-shared key); RSA (authenticated via certificate); and RSA + XAUTH (authenticated via certificate and password).

Configure Address Objects

1. Navigate to **Configure>Objects>Address Objects**.
2. Configure address objects for the local network and the DHCP pool range. The local network is the network to which the client will connect, and the DHCP pool range will be assigned to the clients connecting to the firewall. The default DHCP Pool range is 192.168.73.0/24.

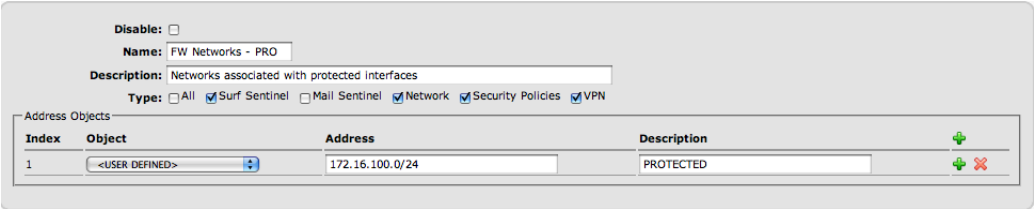

Figure 1.7: *Local Network Address Object*

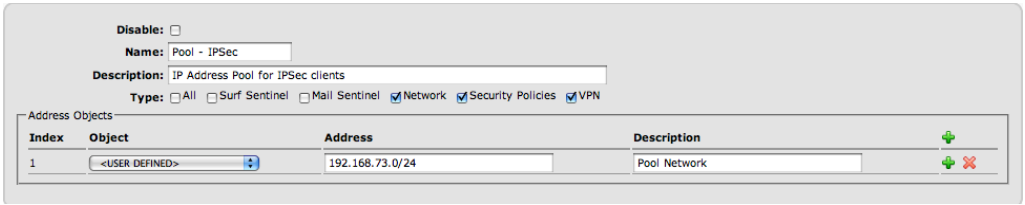

Figure 1.8: *DHCP Pool Address Object*

Configure the Mobile IPSec Client

1. Navigate to **Configure>VPN>Remote Access>IPSec**.
2. Enable the client.
3. Select the IPSec Object specifying encryption and authentication used for the VPN.
4. Define the LOCAL NETWORK the client will connect to.
5. Define the POOL NETWORK representing the DHCP range which will apply to clients using Xauth.
6. Optionally, configure the DNS servers and WINS servers for the client connections.
7. Configure advanced options as necessary.

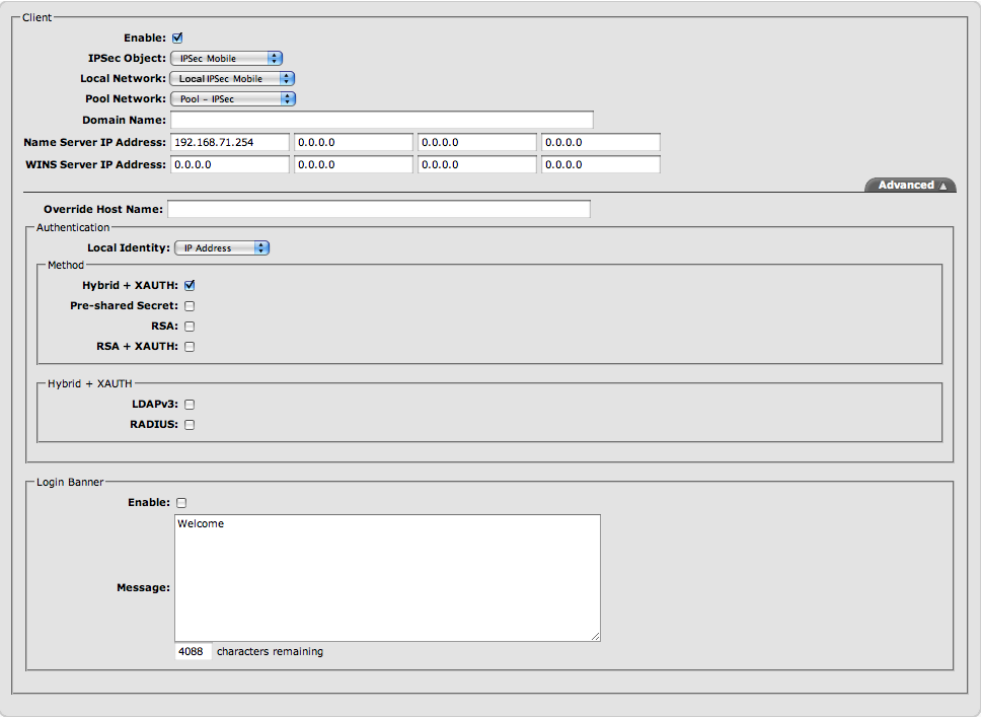

Figure 1.9: *Configuring the IPSec Client*

Table 3: Enable IPSec Client

Field	Default	Description
Client		
Enable	Unchecked	Enable or disable the IPSec Client. Allows dynamic connections to the firewall.
IPSec Object	IPSec Mobile	A selection for the IPSec Object to be used by the IPSec Client. Selecting <* **EDIT** *> allows for the configuration of a new IPSec Object.
Local Network	FW Network - Local	Select the host/subnetwork that should be accessible from the VPN. Select <* **EDIT** *> to define a new address object.
Pool Network	Pool - IPSec	Select the DHCP pool that will be assigned to connecting clients. Select <* **EDIT** *> to define a new address object. Default DHCP range of 192.168.73.0/24.
Domain Name	User Define	Domain assigned to the Mobile IPSec Client.
Name Server IP Address	Blank	DNS server(s) pushed to IPSec Client.
WINS Server IP Address	Blank	WINS server(s) pushed to IPSec Client.

Table 3: Enable IPSec Client		
Field	**Default**	**Description**
Advanced		
Override Host Name	Blank	Allows an administrator to override the default firewall host name, which is configured in Network Settings. Entry can be an IP address or a fully qualified host name. This address will be used to connect to the firewall and should be used whenever the host name assigned to the firewall is not resolvable.
Authentication		
Local Identity	Certificate	Firewall's identity used for mobile IPSec client connections. Options include IP Address, Domain, Email Address and Certificate.
Method		
Hybrid + XAUTH	Checked	Enable or disable Hybrid + XAUTH authentication. Requires User Login and Password
Pre-shared Secret	Unchecked	Enable or disable pre-shared secret authentication. Firewall's local identity must be IP address, Domain or Email address.
RSA	Unchecked	Enable or disable RSA authentication. Requires user to have a signed certificate
RSA + XAUTH	Unchecked	Enable or disable RSA + XAUTH authentication. Requires user to have a signed certificate, and a username and password.
Hybrid + XAUTH		
LDAPv3	Unchecked	Enables LDAP users.
RADIUS	Unchecked	Enables RADIUS users.
Login Banner		
Enable	Unchecked	Enable or disable the login banner message.
Message	Blank	Enter a message to be displayed upon logging into the IPSec Client.

Configure Security Policies

Configure the IPSec security policies based on your corporate security policy. Below is an example of the default IPSec security policies. All access is allowed to internal networks and pings are allowed to the internal protected interfaces.

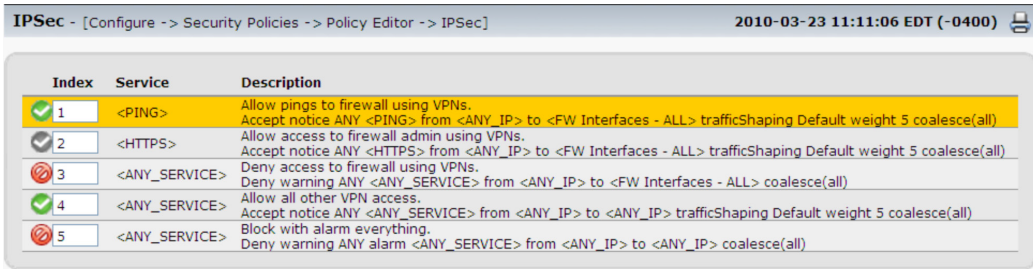

Figure 1.11: *Configuring Security Policies*

PPTP

PPTP Requirements

- GB-OS 5.4.0 or above
- Computer or mobile device which supports PPTP
    - Mobile Devises: iPhone OS 3 or 4.1, Android OS 2.2
- Optional - Radius Server connection configured if using Radius Authentication

Firewall Configuration

Enable PPTP

1. Navigate to **Configure>VPN>Remote Access>PPTP**

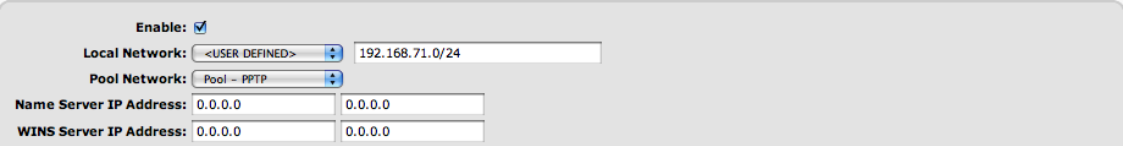

Figure 2.1: *Enable PPTP*

2. Select the ENABLE checkbox to start the PPTP service.
3. The LOCAL NETWORK is the network reachable via PPTP connection. Select an address object or <User Define>.
4. The POOL NETWORK is the range IP address assigned to the host connecting to the PPTP server. The Pool Address must be in a logically different network than any network assigned to the firewall. Default network is 192.168.75.0/24
5. The NAME SERVER IP ADDRESS is the IP address of DNS servers used for resolving names.
6. The WINS SERVER IP ADDRESS is the IP address of the WINS servers.

Authentication

1. Optional: Enable authentication using Radius. Requires Radius server and authentication for Radius configured on the firewall at **Configure>Accounts>Authentication**.

Figure 2.2: *Enabling Radius Authentication*

Advanced

1. Selecting the AUTOMATIC POLICIES checkbox will create an automatic policy to TCP port 1723 and GRE connections to establish the PPTP session with the client.
2. Select the level of encryption to be used for the connection. Options include None, 40, 56, 128 and All.
3. Define the Maximum Transmission Unit (MTU) assigned to the client. Default value is 1460.
4. Define the number of seconds during which a connection will stay connected during periods of inactivity in the TIME OUT field. To prevent timing out on a connection, enter a value of 0.

Figure 2.3: *Configuring Advanced PPTP Options*

Debug

NOTE: This option should only be enabled when troubleshooting a connection.

1. Select CHAT to record dialing and login chat script conversations.
2. Select LCP to record LCP conversations. This is used to set non-default Link Control Protocol options.
3. Select PHASE to record network phase conversations. This is used to determine Local and Remote IP address specifications.

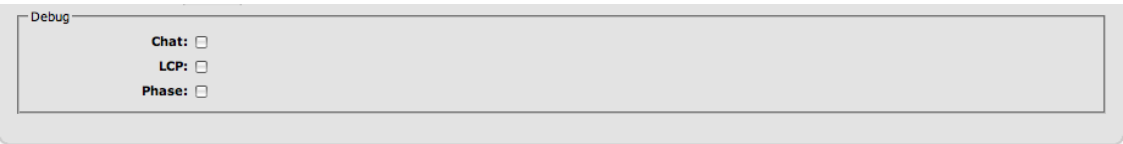

Figure 2.4: *Debugging PPTP*

Create Group

1. Navigate to **Configure>Accounts>Groups**
2. Enter a NAME and DESCRIPTION for the group.
3. Select the PPTP checkbox under Remote Access.
4. If using Radius, enable PPTP on the built in Radius Group - RADIUS Users.

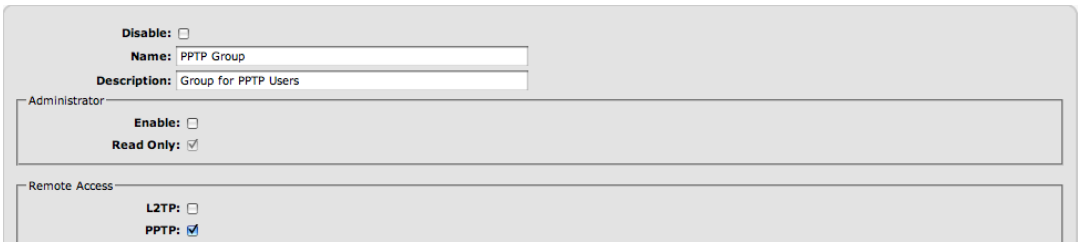

Figure 2.5: *Creating a PPTP Group*

Create User

1. Navigate to **Configure>Accounts>Users**
2. Enter the user's information and leave the DISABLE box unchecked for L2TP/PPTP under Remote Access.
3. Enter the PPTP/L2TP Password for the User.

Note

If using Radius Authentication this step is not required

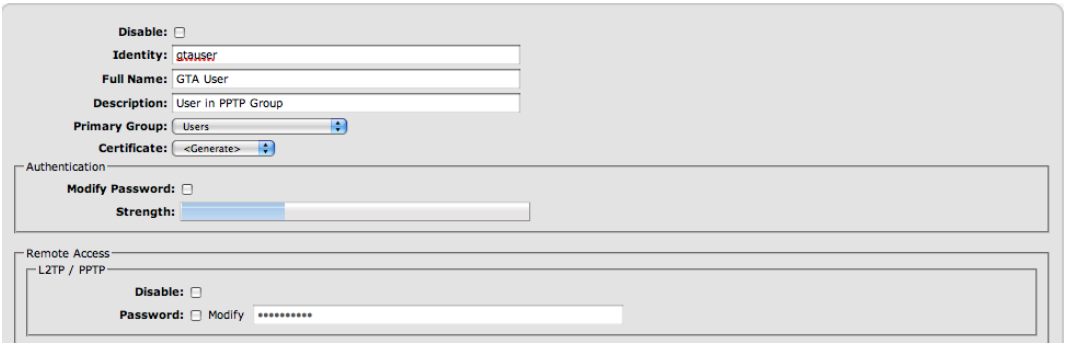

Figure 2.6: *Creating a PPTP User*

Create PPTP Security Policies

1. Create IPSec Security Policies which allow access to internal networks based on corporate security policies in **Configure>Security Policies>Policy Editor>PTPT**.
2. Default policy for GTA firewalls is to Allow IMCP to firewall and Internal networks.
3. Deny Access to firewall Interface for all other services.
4. Allow all access for all other services to internal networks.

Client Configuration

Please see the specific install guide for your mobile device.

Troubleshooting

1. Once the client starts, all Internet access may travel via the VPN to the remote gateway, then to the Internet. The remote firewall must have policies in place to allow Internet Access via the VPN.
2. Confirm pre-shared keys and passwords.
3. No pre-existing tunnel for GRE, PPTP or TCP port 1723 is open on the firewall.
4. Check Log Messages
5. Check firewall for errors acquiring licenses. There may be no more free IPSec Client, L2TP, PPTP Licenses.

L2TP

L2TP Requirements

- GB-OS 5.4.0 or above
- Optional - Radius Server connection configured if using Radius Authentication
- Computer or mobile device which supports L2TP over IPSec
    - Mobile Devises: iPad or iPhone OS 3 or 4.1, Android OS 2.2
- IPSec Remote Access enabled with an IPsec Object referencing support encryption and authentication methods at **Configure>VPN>Remote Access>IPSec**
- Pre-Shared Secret enabled in IPSec Client at **Configure>VPN>Remote Access>IPSec**
- Apple iPhone, iPad, and MAC's - Firewall must use an identity in remote access of IP address at **Configure>VPN>Remote Access>IPSec**
- Phase 1 Security Association Life Time set to 480 minutes
- Phase 2 Security Association Life Time set to 480 minutes if using Android OS

Firewall Configuration

Enable L2TP

1. Navigate to **Configure>VPN>Remote Access>L2TP**
2. Select the Enable checkbox to start the L2TP service.
3. In Interface, specify the interface on which to access connections.
4. The Local Network is the network reachable via L2TP connection. Select an address object or <User Define>.
5. The Pool Network is the range IP address assigned to the host connecting to the L2TP server. The Pool Address must be in a logically different network than any network assigned to the firewall. Default network is 192.168.75.0/24
6. The Name Server IP Address is the IP address of DNS servers used for resolving names.
7. The WINS Server IP Address is the IP address of the WINS servers.

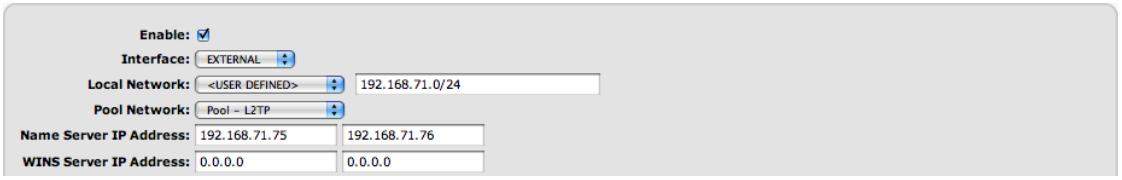

Figure 3.1: *Enabling L2TP*

Authentication

1. Pre-Shared Secret is the secret shared with uses for L2TP over IPSec. This will be same for all users.
2. Optional: Enable authentication using Radius. Requires Radius server and authentication for Radius configured on the firewall at **Configure>Accounts>Authentication**.

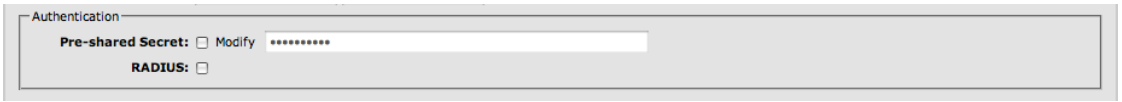

Figure 3.2: *Enabling L2TP Authentication*

Advanced

1. Selecting the Automatic Policies checkbox will create an automatic policy to TCP port 1723 and GRE connections to establish the PPTP session with the client.
2. Define the Maximum Transmission Unit (MTU) assigned to the client. Default value is 1460.
3. Define the number of seconds during which a connection will stay connected during periods of inactivity in the Time Out field. To prevent timing out on a connection, enter a value of 0.

Figure 3.3: *L2TP Advanced Options*

Debug

NOTE: This option should only be enabled when troubleshooting a connection.

1. Select Chat to record dialing and login chat script conversations.
2. Select LCP to record LCP conversations. This is used to set non-default Link Control Protocol options.
3. Select Phase to record network phase conversations. This is used to determine Local and Remote IP address specifications.

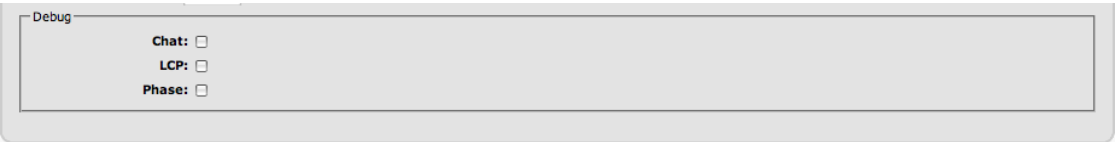

Figure 3.4: *Debugging L2TP*

Configure Encryption Object

1. Navigate to **Configure>Objects>Encryption Objects** and create an Encryption Object for Phase 2 with no PFS.
2. Set the Encryption Method to ES-128
3. Set the Hash Algorithm to Sha1
4. Set the Key Group to None

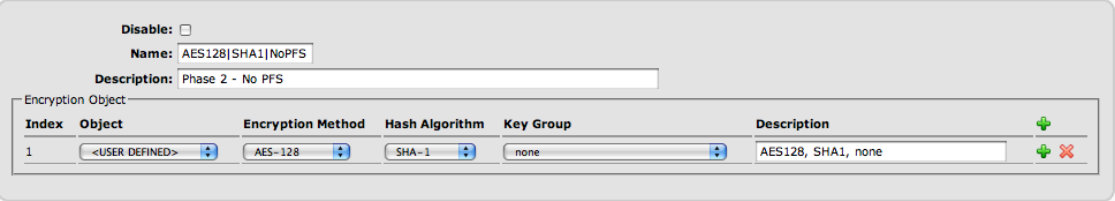

Figure 3.5: *Configuring Encryption Objects for L2TP*

Configure IPSec Object

1. Navigate to **Configure>Objects>IPSec Objects** and create an IPsec Object referencing the Encryption Objects created above.
2. In Phase I, set the following:
   - Exchange Mode: Aggressive
   - Encryption: Select the built in Object<DES3,SHA1,grp2>
   - NAT-T: Automatic
   - Lifetime: 480 minutes
   - DPD Interval: 30 seconds

3. In Phase 2, set the following:
   - Encryption: <Phase 2 object created above>
   - Lifetime: 480 minutes

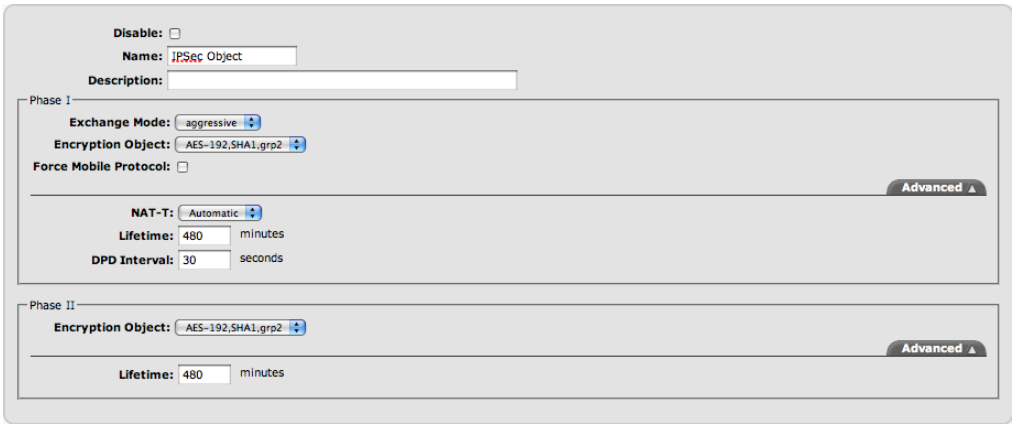

Figure 3.6: *Configuring IPSec Objects for L2TP*

Enable Remote Access

1. Navigate to **Configure>VPN>Remote Access>IPSec**
2. Select the IPSec Object created above.
3. Under Advanced, the Pre-Shared Secret must be enabled.

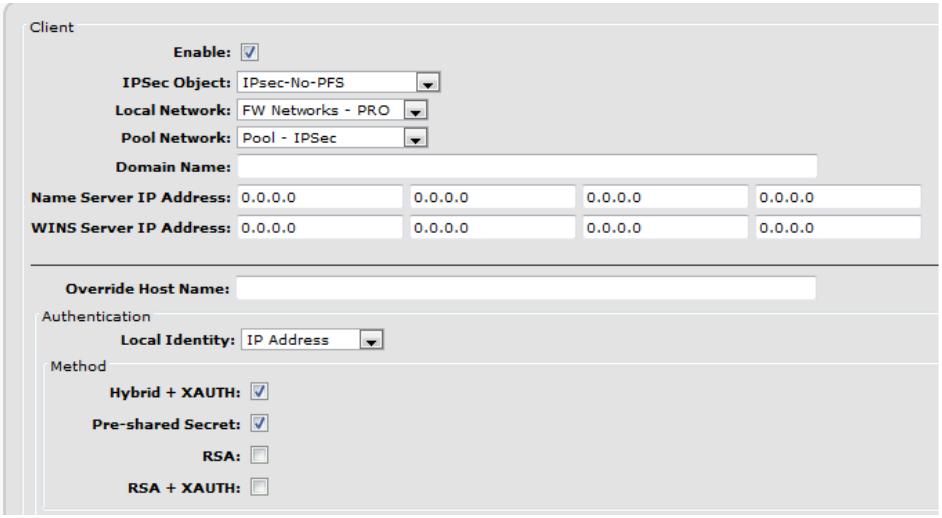

Figure 3.7: *Enabling Remote Access*

Create Group

1. Navigate to **Configure>Accounts>Groups**
2. Enter a NAME and DESCRIPTION for the group.
3. Select the L2TP checkbox under Remote Access.
4. If using radius enable L2TP on the built in Radius Group - RADIUS Users.

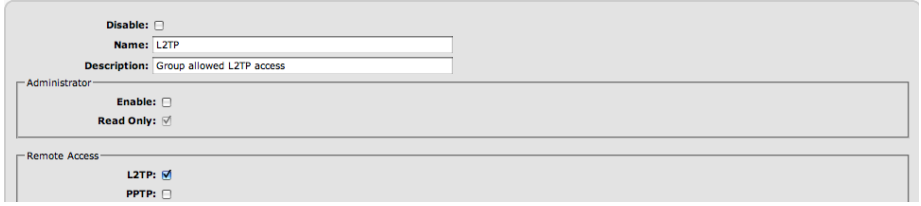

Figure 3.8: *Creating a Group for L2TP*

Create User

1. Navigate to **Configure>Accounts>Users**
2. Enter the user's information and leave the DISABLE box unchecked for L2TP/PPTP under Remote Access.
3. Enter the PPTP/L2TP Password for the User.

Note

If using Radius Authentication this step is not required

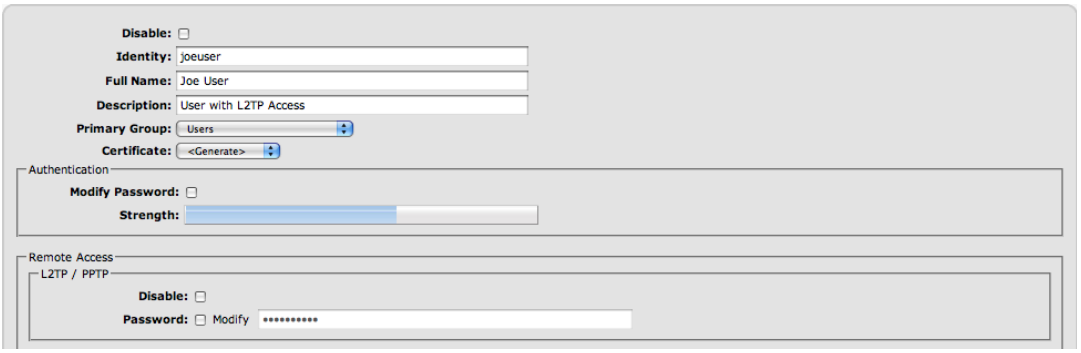

Figure 3.9: *Creating a User for L2TP*

Create IPSec Security Policy

1. Navigate to **Configure>Security Policies>Policy Editor>VPN> IPSec** and create IPsec Policy to Accept L2TP connections

Figure 3.10: *Create an IPSec Policy for L2TP*

Create L2TP Security Policy

1. Create IPSec Security Policies which allow access to internal networks based on corporate security policies in **Configure>Security Policies>Policy Editor>L2TP**.
2. Default policy for GTA firewalls is to Allow IMCP to firewall and Internal networks.
3. Deny Access to firewall Interface for all other services.
4. Allow all access for all other services to internal networks.

Client Configuration

Please see the specific install guide for your mobile device.

Troubleshooting

1. Once the client starts, all Internet access may travel via the VPN to the remote gateway, then to the Internet. The remote firewall must have policies in place to allow Internet Access via the VPN.
2. Confirm pre-shared keys and passwords.
3. MAC's, iPhones, iPads, and Androids require firewall identity to be an IP address for client connections.
4. No pre-existing tunnel for L2TP is in place or IPSec over riding the firewall L2TP server.
5. Check Log Messages
6. L2TP Client shows as connected. However, system cannot pass data. Check firewall for errors acquiring licenses. There may be no more free IPSec Client, L2TP, PPTP Licenses.
7. Clients will establish an IPSec Connection to the firewall over which the L2TP connection will be established. Confirm an IPSec connection for client is displayed in **Monitor>Activity>VPN> IPSec Tunnels**.
8. Once a L2TP/IPSec connection is established, an authenticated user will be displayed in **Monitor>Activity >Accounts>Authenticated.**

L2TP Recommended Encryption Object Configuration

The following is the recommended encryption object configuration to support maximum number of different mobile devices:

	Encryption	Hash	Key Group	Lifetime (seconds)
Phase 1	3DES	SHA1	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
Phase 2	AES128	SHA1	NONE (No PFS)	28,800 (480 minutes)

L2TP Tested Encryption and Authentication Method (by device)

Phase 1

	Encryption	Hash	Key Group	Lifetime (seconds)
WIN7	3DES	SHA1	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
WIN7	3DES	SHA1	Diffie-Hellman group 14 (2048bits)	28,800 (480 minutes)
WIN7	AES128	SHA1	Diffie-Hellman group 14 (2048bits)	28,800 (480 minutes)
Android 2.2	3DES	SHA1	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
Android 2.2	3DES	MD5	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
Android 2.2	DES	SHA1	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
Android 2.2	DES	MD5	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
Android 2.2	AES128	SHA1	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
Android 2.2	AES128	MD5	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
iPhone 3	3DES	SHA1	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)
iPhone 4.1	3DES	SHA1	Diffie-Hellman group 2 (1024 bits)	28,800 (480 minutes)

Phase 2

	Encryption	Hash	Key Group	Lifetime (seconds)
WIN7	3DES	SHA1	NONE (No PFS)	3,600 (60 minutes)
Android	3DES	SHA1	NONE (No PFS)	28,800 (480 minutes)
Android	AES128	SHA1	NONE (No PFS)	28,800 (480 minutes)
iPhone 3	AES128	SHA1	NONE (No PFS)	3,600 (60 minutes)
iPhone 4.1	AES128	SHA1	NONE (No PFS)	3,600 (60 minutes)

Technical Support

GTA includes 30 days "up and running" installation support from the date of purchase. See GTA's Web site for more information. GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local Authorized GTA Channel Partner.

Tel: +1.407.380.0220 **Email:** support@gta.com

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks & Copyrights

GB-OS, Surf Sentinel, Mail Sentinel and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. GB Commander is a trademark of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at http://oss.software.ibm.com/icu4j/.

Some products include software developed by the OpenSSL Project (http://www.openssl.org/).

Mailshell and Mailshell Anti-Spam is a trademark of Mailshell Incorporated. Some products contain technology licensed from Mailshell Incorporated.

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • **Fax**: +1.407.380.6080 • **Web**: http://www.gta.com • **Email**: info@gta.com